AD-A208 623

ICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

RITY CLASSIFICATION

1b. RESTRICTIVE MARKINGS

SSIFICATION AUTHORITY

3. DISTRIBUTION/AVAILABILITY OF REPORT
Approved for public release; distribution unlimited.

TION/DOWNGRADING SCHEDULE

RGANIZATION REPORT NUMBER(S)

5. MONITORING ORGANIZATION REPORT NUMBER(S)
AFOSR-TR- 89-0745

6a. NAME OF PERFORMING ORGANIZATION
University of Southern California
Electrical Engineering Systems

6b. OFFICE SYMBOL (If applicable)

7a. NAME OF MONITORING ORGANIZATION
AFOSR

6c. ADDRESS (City, State, and ZIP Code)
Los Angeles, CA 90007

7b. ADDRESS (City, State, and ZIP Code)
BLDG 410
BAFB DC 20332-6448

8a. NAME OF FUNDING/SPONSORING ORGANIZATION
AFOSR

8b. OFFICE SYMBOL (If applicable)

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
AFOSR 75-2798

8c. ADDRESS (City, State, and ZIP Code)
BLDG 410
BAFB DC 20332-6448

10. SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT ACCESSION NO.
61102F	2304	A6	

11. TITLE (Include Security Classification)
FAST DIGITAL CORRELATIONS AND TRANSFORMS USING FINITE FIELD TECHNIQUES

12. PERSONAL AUTHOR(S)
I.S. Reed

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
Final	FROM _____ TO _____	December 1979	8

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	

19. ABSTRACT (Continue on reverse if necessary and identify by block number)
The research was principally in the following four areas--Finite fields in digital signal processing, transorm decoders for correcting both errors and erasures of the Reed-Solomon code, xray 3-d reconstruction, and a fast two dimensional convolution by the polynomial transorm.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS

21. ABSTRACT SECURITY CLASSIFICATION
unclassified

22a. NAME OF RESPONSIBLE INDIVIDUAL

22b. TELEPHONE (Include Area Code)
767-5025

22c. OFFICE SYMBOL
NM

DD Form 1473, JUN 86 Previous editions are obsolete. SECURITY CLASSIFICATION OF THIS PAGE

FAST DIGITAL CORRELATIONS AND TRANSFORMS USING FINITE FIELD TECHNIQUES

Five Years Technical Progress Report

on

Grant AFOSR 75-2798

In the past five years, the following four areas have been considered under the Grant AFOSR 75-2798 of the U.S. Air Force office of Scientific Research.

(1) Use the Finite Field to Perform Digital Signal Processing

(a) Fast Fourier Transform over Finite Fields

The fast Fourier transform over the finite field is developed to compute one-dimensional convolutions [1-27]. One advantage of such a transform over the usual discrete Fourier transform is that this new transform uses only integer arithmetic. In addition filtering operations or convolutions without round-off error can be obtained, using this transform. Such a transform is applied to compute the two-dimensional convolution for imaging, processing [6] and to compute the discrete Fourier transform [12,15].

(b) Recursive Filters over Finite Fields

Recursive filter design techniques are developed for finite impulse filters, using finite fields. Such recursive finite field filters do not have the accumulation of round-off or truncation error one expects in recursive computations [27,28].

(2) Transform Decoder for Correcting Both Errors and Erasures of the Reed-Solomon Code

A fast transform technique over a finite field is developed to encode and decode the Reed-Solomon code [29-44]. It is demonstrated that the transform decoder for decoding errors and erasures of the (255,223,33) Reed-Solomon code over GF(2^8) is between 3 and 7 times faster than the standard Reed-Solomon decoder, developed previously by NASA [39]. If such a Reed-Solomon code is concatenated with a Viterbi decoded convolutional code it can be used to reduce the signal-to-noise ratio required to meet the specified bit-error rate for deep space applications. It is shown [34,35] also that such transform decoder for Reed-Solomon codes can be used in multiple-user communication systems.

(3) X-Ray 3-D Reconstruction

In computer tomography, the convolution technique utilized the convolution of the cross-sectional projection of an $|\omega|$-filter. The 2-D section of an object is then reconstructed by averaging these convolutions over all projections at all angles from 0 to π. [45-51].

A new class of band-pass $|\omega|$-filters is developed to reduce X-ray dosage and to enhance the edge of reconstructed pictures [50,51]. Weiner Filtering is used to improve the image quality of an object in the 3-Dimensional reconstruc-

tion by a weighted average of successive overlapping two-dimensional sections of the object [49].

(5) A Fast Two-Dimensional Convolution by the Polynomial Transform

A fast algorithm is developed to compute two-dimensional convolutions of an array of $d_1 x d_2$ complex number points, where $d_2 = 2^m$ and $d_1 = 2^{m-r+1}$ for some $1 \leq r \leq m$. This new algorithm requires fewer multiplications and about the same number of additions as the conventional FFT method for computing the two-dimensional convolution. It also has the advantage that the operation of transposing the matrix of data can be avoided. [53]

REFERENCES

The following references are articles and Ph.D dissertations written during this Five Year period:

1. T. K. Truong, "The Application of Finite Fields to Digital Filters," Ph.D. Dissertation, University of Southern California, January 1976.

2. I. S. Reed and T. K. Truong, "The Use of Finite Fields to Compute Convolutions," IEEE Trans. on Inform. Theory, Vol. IT-21, No. 2, March 1975.

3. I. S. Reed and T. K. Truong, "Complex Integer Convolutions Over a Direct Sum of Galois Fields," IEEE Trans. on Inform. Theory, Vol. IT-21, No. 2, November 1975.

4. S. W. Golomb, I. S. Reed and T. K. Truong, "Integer Convolutions Over the Finite Field GF($3 \cdot 2^n+1$)," SIAM Journal on Applied Mathematics, March 1977.

5. I. S. Reed and T. K. Truong, "Convolutions Over Residue Classes of Quadratic Integers," IEEE Trans. on Inform. Theory, Vol. IT-22, No. 4, July 1976.

6. I. S. Reed, T. K. Truong, Y. S. Kwoh and E. L. Hall, "Image Processing by Transforms Over a Finite Field," IEEE Trans. on Computers, Vol. C-26, No. 9, September 1976.

7. I. S. Reed, Y. S. Kwoh, T. K. Truong, E. L. Hall, "X-Ray Reconstruction by Finite Field Transforms," IEEE Trans. on Nuclear Science, Vol. NS-24, No. 1, February 1977.

8. K. Y. Liu, I. S. Reed and T. K. Truong, "Fast Number-Theoretic Transforms for Digital Filtering," Electronic Letters, Vol. 12, No. 24, November 1976.

9. K. Y. Liu, I. S. Reed and T. K. Truong, "Fast Algorithm for Complex Integer Transforms," IEEE Trans. on Acoustics, Speech, and Signal Processing, Vol. ASSP-25, No. 5, October 1977.

10. I. S. Reed and T. K. Truong, "Convolutions Over Quartic Integer Residue Classes," The Proceedings of the International Conference on Information Sciences and Systems, Patras, Greece, August 19-24, 1976.

11. I. S. Reed and T. K. Truong, "Correction to Convolutions Over Residue Classes of Quadratic Integers," IEEE Trans. Inform. Theory, Vol. IT-23, No. 4, July 1977.

12. I. S. Reed and T. K. Truong, "A Fast DFT Algorithm Using Complex Integer Transforms," Electronic Letters, Vol. 14, No. 6, March 1978.

13. I. S. Reed and T. K. Truong, "A Fast Computation of Complex Convolution Using a Hybrid Transform," IEEE Trans. Acoustics, Speech, and Signal Processing, Vol. ASSP-26, No. 6, December 1978.

14. I. S. Reed and T. K. Truong, "Fast Mersenne-Prime Transforms for Digital Filtering," Proceeding IEE, Vol. 125, No. 5, May 1978.

15. I. S. Reed and T. K. Truong, "A Fast and New Hybrid Algorithm for Computing the Discrete Fourier Transform," IEEE Trans. on Computers, Vol. C-28, No. 7, July 1979, pp. 487-492.

16. I. S. Reed, and T. K. Truong, "Addendum to Fast Algorithm for Computing Complex Number-Theoretic Transforms," Electronic Letters, Vol. 14, No. 7, March 1978.

17. I. S. Reed, T. K. Truong and R. L. Miller, "Correction to Fast Algorithm for Computing Complex-Theoretic Transform," Electronic Letters, Vol. 14, No. 13, June 1978.

18. I. S. Reed, T. K. Truong and R. L. Miller, "A Theorem for Computing Primitive Elements in the Field of Complex Integers Mersenne Prime," (to be published) IEEE Trans. Acoustics, Speech, and Signal Processing.

19. I. S. Reed, T. K. Truong and R. L. Miller, "A Fast Algorithm for Computing a Primitive 2^{p+1} p-th Root of Unity in $GF((2^p-1)^2)$," Electronic Letters, Vol. 14, No. 15, 20th July, 1978.

20. I. S. Reed, T. K. Truong and R. L. Miller, "Correction to Fast Mersenne Prime Transforms for Digital Filters," Proceedings IEE, Vol. 126, No. 2, February 1979.

21. I. S. Reed, T. K. Truong and R. L. Miller, "A Simple Method for Computing Elements of order $2^k \cdot n$, where $n|2^{p-1}-1$ and $2 \leq k \leq p+1$ in $GF((2^p-1)^2)$," Electronic Letters, No. 14, pp. 697-698, 1978.

22. I. S. Reed, T. K. Truong and R. L. Miller, "Correction to Simple Method for Computing Elements of Order $2^k \cdot n$, where $n|2^{p-1}-1$ and $2 \leq k \leq p+1$, in $GF[(2^{p-1}-1)^2]$, Electronic Letters, Jan. 18, 1979.

23. I. S. Reed, T. K. Truong and R. L. Miller, "A New Algorithm for Computing Primitive Elements in the Field of Gaussian Complex Integers Modulo a Mersenne Prime," IEEE Trans. on Acoustics Speech and Signal Processing, Vol. ASSP-27, No. 5, Oct. 1979.

24. S. W. Golomb, "Properties of the Sequence $3 \cdot 2^n+1$," Mathematics of Computations, Vol. 30, No. 135, July 1976.

25. S. W. Golomb, "Cyclotomic Polynomials and Factorization Theorems," American Mathematical Monthly, Vol. 85, No. 9,

26. S. W. Golomb, "Obtaining Specified Irreducible Polynomials over Finite Field," SIAM Appl. Math.

27. H. Murakami and I. S. Reed, "Recursive Realization of Finite Impulse Filters, Using Finite Field Arithmetic," IEEE Trans. on Inform. Theory, Vol. IT-23, No. 2, March 1977.

28. H. Murakami, "Theory and Application of Digital Signal Processing over a Finite Ring," Ph.D. Dissertation, University of Southern California, June 1977.

29. K. Y. Liu, "Efficient Digital Transform Algorithms and Architectures for Signal Processing and Error Correcting Codes," Ph.D. Dissertation, University of Southern California, June 1977.

30. K. Y. Liu, I. S. Reed and T. K. Truong, "High-Radix Transforms for R-S Codes Over Fermat Primes," IEEE Trans. Inform. Theory, Vol. IT-23, No. 6, November 1977.

31. I. S. Reed, T. K. Truong and L. R. Welch, "The Fast Decoding of Reed-Solomon Codes Using Fermat Theoretic Transforms," IEEE Trans. Inform. Theory, Vol. IT-24, No. 4, July 1978.

32. I. S. Reed, R. A. Scholtz, T. K. Truong and L. R. Welch, "The Fast Decoding of Reed-Solomon Codes Using Fermat Theoretic Transforms and Continued Fractions," IEEE Trans. on Inform. Theory, Vol. IT-24, No. 1, January 1978.

33. Y. S. Kwoh, I. S. Reed and T. K. Truong, "A Generalized . - Filter for 3-D Reconstruction" IEEE Trans. on Nuclear Science, Vol. NS-24, No. 5, October 1977.

34. H. Murakami, I. S. Reed and L. R. Welch, "Transform Decoder of Reed-Solomon Codes for Multiple-User Communication Systems Using a Direct Sum of Galois Fields," IEEE Trans. Inform. Theory, Vol. IT-28, No. 9, November 1977.

35. H. Murakami and I. S. Reed, "Multi-Channel Convolutional Coding Systems Over a Direct Sum of Galois Fields," IEEE Trans. on Inform. Theory, Vol. IT-24, No. 2, March 1978.

36. I. S. Reed, T. K. Truong, B. D. L. Mulhall, J. S. L. Wong and B. Benjauthrit, "Review of Finite Fields, Applications to Fast Fourier Transforms and Reed-Solomon Coding," in Jet Propulsion Laboratory Technical Report, Pasadena, California, July 1977.

37. I. S. Reed, T. K. Truong and B. Benjauthrit, "On Decoding of Reed-Solomon Codes Over GF(32) and GF(64) Using the Transform Techniques of Winograd," National Telecommunications Conference, Birmingham, Alabama, December 1978.

38. I. S. Reed and T. K. Truong, "A Simple Proof of the Continued Fraction Algorithm by Using Continued Fraction Approximations," Proceedings IEE, Vol. 125, No. 12, December 1978.

39. I. S. Reed, R. L. Miller and T. K. Truong, "An Efficient Program for Decoding the (255,233) Reed-Solomon Code over GF(2^8) with both Errors and Erasures Using Transform Decoding," to be published in Proc. IEE.

40. R. L. Miller, I. S. Reed and T. K. Truong, "Simplified Algorithm for Correcting both Errors and Erasures of Reed-Solomon Codes," Proc. IEE, Vol. 126, No. 10, October 1979.

41. I. S. Reed, T. K. Truong and R. L. Miller, "Decoding of B.C.H. and R.S. Codes with Errors and Erasures Using Continued Fractions," Electronics Letters, 16th August 1969, Vol. 15, No. 17, pp. 542-544.

42. T. K. Truong, R. L. Miller and I. S. Reed, "Fast Technique for Computing Syndromes of B.C.H. and Reed-Solomon Codes," Electronics Letters, 25th October, 1979, Vol. 15, No. 22, pp. 720-727.

43. R. L. Miller, T. K. Truong and I. S. Reed, "A Fast Algorithm for Encoding the (255,223) Reed-Solomon Code over GF(2^{∞})", Electronics Letters, 13th March, 1980, Vol. 16, No. 6.

44. R. L. Miller, I. S. Reed and T. K. Truong, "The Probability of Incorrectly Decoding Errors and Erasures of Reed-Solomon Code Words," Submitted to Proc. IEE.

45. C. M. Chang, "3-D Reconstruction and the Technique of X-Ray Computerized Tomography," Ph.D. Dissertation, July 1979.

46. Y. S. Kwoh, I. S. Reed and T. K. Truong, "Back Projection Speed Improvement for 3-D Reconstruction" IEEE Trans. on Nuclear Science, Vol. NS-24, No. 5, October, 1977.

47. I. S. Reed, T. K. Truong, C. M. Chang and Y. S. Kwoh, "3-D Reconstruction for Diverging X-Ray Beams," IEEE Trans. on Nuclear Science, Vol. NS-25, No. 3, June 1978, pp. 1006-1010.

48. I. S. Reed, W. V. Glenn, Y. S. Kwoh, T. K. Truong and C. M. Chang, "A Clinical Experience with Low Dose Algorithms," Scientific Program for the International Symposium and Course on Computed Tomography, April 16-20, 1979, Las Vegas, Nevada.

49. I. S. Reed, W. V. Glenn, G. M. Chang, T. K. Truong, and C. M. Chang, "Wiener Filtering of Successive Overlapping Sections of An X-Ray Reconstruction," IEEE Transactions on Biomedical Engineering, Vol. BME-27, No. 2, February, 1979.

50. I. S. Reed, W. V. Glenn, Y. S. Kwoh, T. K. Truong and C. M. Chang, "X-Ray Reconstruction of the Spinal Cord Using Bone Cancellation," (to be published) IEEE Transactions on Biomedical Engineering.

51. I. S. Reed, W. V. Glenn, C. M. Chang, T. K. Truong and Y. S. Kwoh, "Dose Reduction in X-Ray Computed Tomography Using a Generalized Filter," IEEE Trans. on Nuclear Science, Vol. NS-26, No. 2, April 1979.

52. K. Y. Liu, I. S. Reed and T. K. Truong, "A New Fast Algorithm for Computing Complex Number-Theoretic Transforms," Electronic Letters, Vol. 13, No. 10, 12th May, 1977.

53. T. K. Truong, I. S. Reed, R. Lipes and C. Wu, "On the Application of a Fast Polynomial Transform and the Chinese Remainder Theorem to Compute a Two-Dimensional Convolution," Submitted to IEEE Trans. on Acoustics, Speech and Signal Processing.